(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC MT NL PL PT RO SE SI SK TR

(30) Priority: **18.12.2006 CN 200610105203**

(71) Applicant: **China Iwncomm Co., Ltd.**
Xi'an, Shaanxi 710075 (CN)

(72) Inventors:
• **LAI, Xiaolong**
Xi'an, Shaanxi 710075 (CN)

• **CAO, Jun**
Xi'an, Shaanxi 710075 (CN)
• **TIE, Manxia**
Xi'an, Shaanxi 710075 (CN)
• **ZHANG, Bianling**
Xi'an, Shaanxi 710075 (CN)

(74) Representative: **Heinze, Ekkehard et al**
Meissner, Bolte & Partner GbR
Widenmayerstrasse 48
80538 München (DE)

(54) **A 3-ELEMENT STRUCTURE PEER ACCESS CONTROL METHOD**

(57)   A 3-element structure peer access control method that realized safe bidirectional authentication between terminal and network is provided. On the basis of 2-element and 3-entity structure access control method, said method realizes authorization function in the access controller, and realizes authentication protocol function between terminal and access controller, makes it possible that terminal, access controller and server join authentication, one-off credit relationship between terminal and access controller is established. According to said method the problems such as the flexibility restriction of access form in 2-element and 2-entity structure access control method in prior art is solved, and such as expandability of access controller amount is solved. The problems such as complexity in the procedure of credit relationship establishment in 2-element and 3-entity structure access control method in prior art is solved. And the safety and authentication protocol independence without changing network structure are achieved.
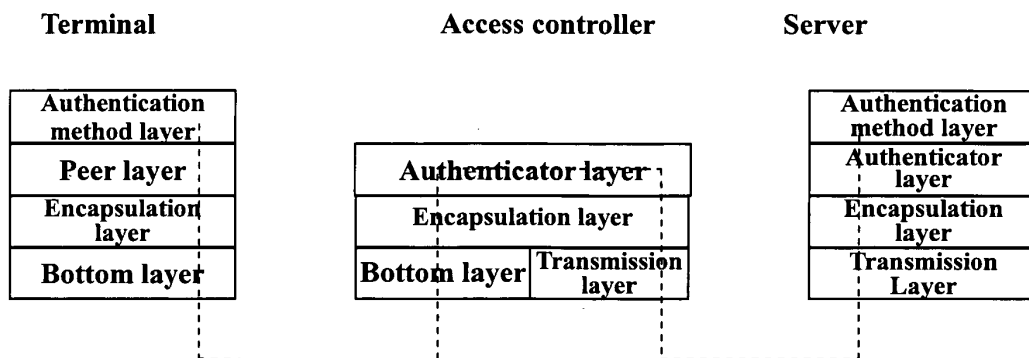
Fig.3

EP 2 124 417 A1

Description

[0001]   This application claims the priority of Chinese Patent Application No. 200610105203.2, filed on December 18, 2006 with the Chinese Patent Office and titled "Peer-to-Peer Access Control Method of Triple-unit Structure", the contents of which are incorporated herein by reference in their entirety.

Field of the Invention

[0002]   The present invention relates to a network access control method, and particularly to a peer-to-peer access control method of a triple-unit structure.

Background of the Invention

[0003]   The basic function of a network is to provide various types of terminals with network services. Although a terminal may be physically connected to a network, the terminal connected to the network is not always an authorized legal terminal, and the network connected by the terminal is not always its required network. Thus, before the terminal communicates with the network, the terminal and the network need authentication and authorization functions to mutually authenticate the legality of the peer party therebetween, i.e. bidirectional access control between the terminal and the network is required, so as to ensure the security of the communication.

[0004]   Figure 1 is a diagram illustrating bidirectional access control between a terminal and a network. A terminal 1 accesses a network 4 via an access controller 3, and before the terminal 1 begins to use the resources of the network 4, it is required to complete access control 2 between the terminal 1 and the access controller 3, i.e.:

[0005]   1. The access controller checks whether the terminal 1 has the right of accessing the network 4, i.e. authenticates the terminal 1; and

[0006]   2. The terminal 1 checks whether the access controller 3 is a legal device to avoid data being intercepted, i.e. authenticates the network 4.

[0007]   In the authentication, it is required to use the concepts of entity and unit. Specifically, an entity refers to a functional body which may accomplish a particular function in the network structure and can exist independently, and is typically implemented using an independent device; and a unit refers to a functional body which may have an authentication function in the network access authentication. In the network, the entity is a unit if it has the authentication function; and it is not a unit if it does not have the authentication function.

[0008]   Based on the different number of entities which participate in the authentication, there are two types of network structure for implementing the bi-directional authentication between the terminal and the network. RFC3748 Extensible Authentication Protocol (EAP) contains description as follows:

[0009]   The network structure of the first type is the dou-

ble-unit double-entity structure as shown in Figure 2, which includes a terminal and an access controller, where the terminal corresponds to the first entity and the access controller corresponds to the second entity. Specifically, the terminal, corresponding to the first unit, has an authentication credential, an authentication function, and a function for controlling whether to access the network; and the access controller, corresponding to the second unit, has an authentication credential, an authentication function, and a function for controlling the access of the terminal according to the result of the authentication. In this network structure, the terminal and the access controller both have authentication functions, thus supporting bidirectional authentication.

[0010]   However, there is no authentication server in the double-unit double-entity structure, which leads to significantly limited flexibility. In addition, there are typically a large number of terminals, and if there is also a large number of access controllers, the relationship between the terminals and the access controllers may be many-to-many, and the management may be very difficult. Therefore, the structure of this type is typically used in the case that there is a limited number of access controllers, and the implementation is very limited.

[0011]   The network structure of the second type is the double-unit triple-entity structure as shown in Figure 3, which includes a terminal, an access controller and a server, respectively corresponding to the first entity, the second entity and the third entity. Specifically, the terminal, corresponding to the first unit, has an authentication credential, an authentication function, and a function for controlling whether to access the network; the access controller has a function for controlling the access of the terminal according to the result of the authentication, and has no authentication function; and the server, corresponding to the second unit, has an authentication credential and an authentication function. The double-unit triple-entity structure is also called a Pass-through mode. In this network structure, the terminal and the server both have authentication functions, but the access controller has no authentication function, thus the structure of this type supports bidirectional authentication by using the second entity as an intermediate of the third entity.

[0012]   In the double-unit triple-entity structure, the access controller is virtual. The authentication is only carried out between the terminal and the server, and the relationship with multiple terminals being corresponding to multiple access controllers is evolved into a relationship with multiple terminals being corresponding to a server, i.e. a trust relationship A is established between them. But finally, it is required to establish a trust relationship B between the terminal and the access controller, thus a transfer of the trust relationships, i.e. to transfer from the trust relationship A to the trust relationship B, must be carried out safely. The transfer of the trust relationships is completed by sending a key from the server to the access controller. However, if the key leaks, the security of the network may be significantly influenced.

Therefore, in order to avoid this problem, a trust relationship C and a safe channel have to be established between the access controller and the server. Upon reception of the key by the access controller, the terminal and the access controller have to confirm the trust relationship B. Hence, it is required to relay the trust relationships three times to complete the establishment of the trust relationship between the terminal and the access controller. However, to relay the trust relationships multiple times may not only lead to complicated authentication but also influence the security of the network, thus should be avoided.

Summary of the Invention

[0013]   The present invention provides a peer-to-peer access control method of a triple-unit structure for safely implementing bidirectional authentication between the terminal and the network, which not only solves the technical problems of the access control method of the existing double-unit double-entity structure that the access flexibility is limited and the extension of the number of the access controllers is inconvenient, but also solves the technical problems of the existing access control method of the double-unit triple-entity structure that the process for establishing the trust relationship is complicated and the security of the network may be influenced.

[0014]   A technical solution of the present invention may include:

[0015]   A peer-to-peer access control method of a triple-unit structure, which includes:

[0016]   implementing, in a subject, a subject function; implementing, in an authenticator, an authenticator function; and implementing, in an authentication server, an authentication server function:

[0017]   setting, in the subject, an authentication method layer of the subject, a peer layer of the subject, an encapsulation layer of the subject and a bottom layer of the subject; setting, in the authenticator, an authentication method layer of the authenticator, an authenticator layer of the authenticator, an encapsulation layer of the authenticator, a bottom layer of the authenticator and a transmission layer of the authenticator; and setting, in the authentication server, an authentication method layer of the authentication server, a peer layer of the authentication server, an encapsulation layer of the authentication server and a transmission layer of the authentication server; and

[0018]   implementing, in the authentication method layer of the subject, a function for carrying out, according to an authentication credential, authentication, and implementing, in the bottom layer of the subject, a function for transmitting data and for controlling, according to a result of the authentication, whether the subject accesses the authenticator; implementing, in the authentication method layer of the authenticator, a function for carrying out, according to an authentication credential, authentication, and implementing, in the bottom layer of the authentica-

tor, a function for controlling, according to a result of the authentication, whether to permit the subject to access the authenticator; and implementing, in the authentication method layer of the authentication server, a function for carrying out, according to an authentication credential, authentication;

[0019]   implementing, in the subject and the authenticator, an authentication protocol function:

[0020]   implementing, in the authentication method layer of the subject together with the authentication method layer of the authenticator, the authentication protocol function;

[0021]   implementing, by the subject and the authenticator, an authentication process:

[0022]   sending, by the authentication method layer of the authenticator, a request message to the authentication method layer of the subject; and sending, by the authentication method layer of the subject, a response message to the authentication method layer of the authenticator to respond to a valid request message; and

[0023]   implementing, upon termination of the authentication, access control:

[0024]   stopping sending, by the authentication method layer of the authenticator when being unable to authenticate the subject according to the response message, the request message and terminating message interaction, and notifying, by the authentication method layer of the authenticator, the bottom layer of the authenticator that the subject is not permitted to access the authenticator; or sending, by the authentication method layer of the authenticator, a failure message to the authentication method layer of the subject, and notifying, by the authentication method layer of the subject, the bottom layer of the subject that the subject is not permitted to access the authenticator; and

[0025]   stopping sending, by the authentication method layer of the authenticator when determining that the authentication is completed successfully according to the response message, the request message and terminating the message interaction, and notifying, by the authentication method layer of the authenticator, the bottom layer of the authenticator that the subject is permitted to access the authenticator; or sending, by the authentication method layer of the authenticator, a success message to the authentication method layer of the subject, and notifying, by the authentication method layer of the subject, the bottom layer of the subject that the subject is permitted to access the authenticator.

[0026]   The request message sent by the authentication method layer of the authenticator to the authentication method layer of the subject contains a type field, which type field is a field used for indicating a type of the request message; and the response message sent by the authentication method layer of the subject to the authentication method layer of the authenticator contains a type field, which type field corresponds to the type field contained in the request message.

[0027]   The above method may further includes the fol-

lowing step:

[0028] maintaining, as required, the interaction of sending the request message by the authentication method layer of the authenticator and responding to the request message by the authentication method layer of the subject.

[0029] The subject may be a terminal; the authenticator may be an access controller; and the authentication server may be a server.

[0030] Another technical solution of the present invention includes:

[0031] A peer-to-peer access control method of a triple-unit structure, which includes:

[0032] implementing, in a subject, a subject function; implementing, in an authenticator, an authenticator function; and implementing, in an authentication server, an authentication server function:

[0033] setting, in the subject, an authentication method layer of the subject, a peer layer of the subject, an encapsulation layer of the subject and a bottom layer of the subject; setting, in the authenticator, an authentication method layer of the authenticator, an authenticator layer of the authenticator, an encapsulation layer of the authenticator, a bottom layer of the authenticator and a transmission layer of the authenticator; and setting, in the authentication server, an authentication method layer of the authentication server, a peer layer of the authentication server, an encapsulation layer of the authentication server and a transmission layer of the authentication server; and

[0034] implementing, in the authentication method layer of the subject, a function for carrying out, according to an authentication credential, authentication, and implementing, in the bottom layer of the subject, a function for transmitting data and for controlling, according to a result of the authentication, whether the subject accesses the authenticator; implementing, in the authentication method layer of the authenticator, a function for carrying out, according to an authentication credential, authentication, and implementing, in the bottom layer of the authenticator, a function for controlling, according to a result of the authentication, whether to permit the subject to access the authenticator; and implementing, in the authentication method layer of the authentication server, a function for carrying out, according to an authentication credential, authentication;

[0035] implementing, in the subject, the authenticator and the authentication server, an authentication protocol function:

[0036] implementing, in the authentication method layer of the subject together with the authentication method layer of the authenticator and together with the authentication method layer of the authentication server, the authentication protocol function;

[0037] implementing, by the subject, the authenticator and the authentication server, an authentication process:

[0038] sending, by the authentication method layer of the authenticator during the message interaction between the authentication method layer of the subject and the authentication method layer of the authenticator, a request message to the authentication method layer of the authentication server, and sending, by the authentication method layer of the authentication server, a response message to the authentication method layer of the authenticator; and

[0039] implementing, upon termination of the authentication, access control:

[0040] stopping sending, by the authentication method layer of the authenticator when being unable to authenticate the subject according to the response message of the authentication method layer of the subject or according to the response message of the authentication method layer of the authentication server, the request message and terminating the message interaction, and notifying, by the authentication method layer of the authenticator, the bottom layer of the authenticator that the subject is not permitted to access the authenticator; or sending, by the authentication method layer of the authenticator, the failure message to the authentication method layer of the subject, and notifying, by the authentication method layer of the subject, the bottom layer of the subject that the subject is not permitted to access the authenticator; and

[0041] stopping sending, by the authentication method layer of the authenticator when determining that the authentication is completed successfully according to the response message of the authentication method layer of the subject or according to the response message of the authentication method layer of the authentication server, the request message and terminating the message interaction, and notifying, by the authentication method layer of the authenticator, the bottom layer of the authenticator that the subject is permitted to access the authenticator; or sending, by the authentication method layer of the authenticator, the success message to the authentication method layer of the subject, and notifying, by the authentication method layer of the subject, the bottom layer of the subject that the subject is permitted to access the authenticator.

[0042] The request message sent by the authentication method layer of the authenticator to the authentication method layer of the subject contains a type field, which type field is a field used for indicating a type of the request message; and the response message sent by the authentication method layer of the subject to the authentication method layer of the authenticator contains a type field, which type field corresponds to the type field contained in the request message; and the request message sent by the authentication method layer of the authenticator to the authentication method layer of the authentication server contains a type field, which type field is a field used for indicating a type of the request message; and the response message sent by the authentication method layer of the authentication server to the authentication method layer of the authenticator contains a type field, which type field corresponds to the type field

contained in the request message.

[0043] The above method may further include the following steps:

[0044] maintaining, as required, the interaction of sending the request message by the authentication method layer of the authenticator and responding to the request message by the authentication method layer of the subject; and

[0045] maintaining, as required, the interaction of sending the request message by the authentication method layer of the authenticator and responding to the request message by the authentication method layer of the authentication server.

[0046] The subject may be a terminal; the authenticator may be an access controller; and the authentication server may be a server.

[0047] When implementing the method of the present invention in the network structure of a specific type, the authentication carried out by the terminal (subject) and the access controller (authenticator) needs assistance of the server. The terminal can communicate with the access controller and cannot communicate with the server, while the access controller can communicate with the terminal and can also communicate with the server. The terminal, the access controller and the server all participate in the authentication, and the trust relationship is established between the terminal and the access controller directly, which renders security very reliable.

[0048] In addition, the method of the present invention may be implemented in a triple-unit structure, but may be compatible to double-unit double-entity structure. In the case that there is no authentication server, the implementation of the method of the present invention is totally compatible to the double-unit double-entity network structure. Therefore, the method of the present invention may be implemented in both the double-entity and the triple-entity structure, which may have full adaptability to the existing network structures.

[0049] Besides, when implementing the method according to the present invention, the authentication protocol layer may use existing authentication protocols, or alternatively new authentication protocols may be devised.

Brief Description of the Drawings

[0050] Figure 1 is a diagram illustrating bidirectional access control between a terminal and a network in the prior art;

[0051] Figure 2 is a diagram illustrating a connection relationship of a network access control system of a double-unit double-entity structure in the prior art;

[0052] Figure 3 is a diagram illustrating a connection relationship of a network access control system of a double-unit triple-entity structure in the prior art;

[0053] Figure 4 is a flowchart illustrating a network peer-to-peer access control method of the present invention;

[0054] Figure 5 a diagram illustrating a connection relationship of a triple-unit triple-entity structure in which the network peer-to-peer access control method of the present invention is implemented; and

[0055] Figure 6 is a flowchart illustrating the method of the present invention being implemented in a specific certificate authentication process.

[0056] Specifically: 1- terminal, 2 - access control, 3 - access controller, 4 - network.

Detailed Description of the Embodiments

[0057] First, the principles of the present invention are described as follows:

[0058] An authentication protocol is a series of steps carried out by two or more participants to complete an authentication. The authentication method layers of the subject, the authenticator and the authentication server are the implementation of the authentication protocol in each of the participants, and they together construct an authentication protocol layer, so as to complete the authentication protocol function.

[0059] In the present invention, the functions of the terminal, the access controller and the server are adjusted, so that the access controller has an authentication credential and an authentication function, and the network structure is changed to triple-unit triple-entity. As shown in Figure 5:

[0060] The first entity/the first unit: the terminal, which has an authentication credential, an authentication function, and a function for controlling whether to access the network.

[0061] The second entity/the second unit: the access controller, which has an authentication credential, an authentication function, and a function for controlling the access of the terminal according to the result of the authentication.

[0062] The third entity/the third unit: the server, which has an authentication credential and an authentication function.

[0063] In this structure, the authentication carried out by the terminal (subject) and the access controller (authenticator) needs assistance of the server (authentication server). The terminal can communicate with the access controller and cannot communicate with the server, while the access controller can communicate with the terminal and can also communicate with the server. The terminal, the access controller and the server all participate in the authentication, and the trust relationship is established between the terminal and the access controller directly, which renders security very reliable.

[0064] If only the subject and the authenticator is required to participate in the authentication protocol, the authentication method layer of the subject together with the authentication layer of the authenticator construct the authentication protocol layer, and complete the authentication protocol function together. If the server is required to participate in the authentication carried out by the sub-

ject and the authenticator, the authentication method layer of the subject together with the authentication layer of the authenticator and together with the authentication layer of the authentication server construct the authentication protocol layer, and complete the authentication protocol function together. They three may run the same authentication protocol. Alternatively, different authentication protocols may be run between any two of them. However, there is essentially an association in the messages between those two of them, so that to achieve the same object, i.e. to complete the authentication between the subject and the authenticator.

[0065] In the art, the concepts of the bottom layer, the transmission layer, the encapsulation layer, the peer layer, the authenticator layer and the authentication method layer are as follows:

[0066] The bottom layer and the transmission layer: the bottom layer and the transmission layer are responsible for transmitting and receiving Triple-unit Extensible Authentication Protocol (TEAP) data frames between the peer and the authenticator. The transmission layer is a logic concept, which means that this layer may be of a technique different from that of the adjacent bottom layer.

[0067] The encapsulation layer: the encapsulation layer transmits and receives the TEAP data packets via the bottom layer, implements repeated-frame detection and retransmission, and transmits messages between the peer layer and the authenticator layer.

[0068] The peer layer and the authenticator layer: the encapsulation layer parses the TEAP data frames and transmits them to the peer layer or the authenticator layer. The peer layer and the authenticator layer parse the received data packets and transmit them to the peer layer or the authenticator layer.

[0069] The authentication method layer: the authentication method layer implements an authentication algorithm, and transmits messages via the peer layer and the authenticator layer.

[0070] Figure 4 is a flowchart illustrating a network peer-to-peer access control method of the present invention. Specifically, a subject function is implemented in the subject, an authenticator function is implemented in the authenticator, an authentication server function is implemented in the server; and a corresponding protocol of the authentication method is implemented in the terminal, the access controller and the server. The specific steps of the method according to the present invention are as follows:

[0071] 401. The access controller sends a request message to the terminal to request starting authentication. The request message has a type field for indicating the type of the request. The type may be Identity, MD5-Chanllenge, etc.;

[0072] 402. The terminal sends a response message to the access controller to respond to the valid request message. The response message contains a type field, which corresponds to the type field contained in the request message;

[0073] 403. According to various authentication methods, the access controller sends a request message to the server if required;

[0074] 404. The server sends a response message to the access controller. The sequence of the request message and the response message may be maintained for a required length;

[0075] 405 - 406. The access controller sends a request message to the terminal, and the terminal sends a response message to the access controller, where the sequence of the request message and the response message may maintain interaction as required. Of course, according to various authentication methods, the terminal may possibly not respond to the request message sent by the access controller.

[0076] 407. The session is maintained until the access controller cannot authenticate the terminal. The access controller may stop sending the request message and terminate the message interaction, and the access controller may send a failure message to the terminal and the access controller does not permit the terminal to access the access controller; or alternatively, the access controller may determine that a successful authentication has been completed, and the access controller may stop sending the request message and terminate the message interaction, or may send a success message to the terminal and the access controller permits the terminal to access the access controller. At this time, the access control between the terminal and the access controller is completed.

[0077] An embodiment of the present invention is implemented in the model of the authentication method defined in the national standard GB15629.11-2003/XG1-2006. The certificate authentication process described in this standard is as shown in Figure 6, and specifically includes the following:

[0078] In Figure 6, the ASUE refers to the Authentication Supplicant Entity, i.e. the terminal, which implements the subject function; the AE refers to the Authenticator Entity, i.e. the access controller, which implements the authenticator function; and the ASE refers to the Authentication Service Entity, i.e. the server, which implements the authentication server function. The authentication method described in this standard needs to be implemented in all the ASUE, the AE and the ASE, which complies with and thus may be implemented in the model of the method according to the present invention. Specifically:

[0079] 601. The AE sends a request message to the ASUE;

[0080] 602. The ASUE sends a response message to the AE;

[0081] 603. The AE sends a request message to the ASE;

[0082] 604. The ASE sends a response message to the AE; and

[0083] 605. The AE sends a request message to the ASUE; the ASUE receives the request message, and

does not need to send a response message; and the AE stops sending messages.

[0084] For the definitions of the specific fields contained in the message, reference can be made to the definitions in the national standard GB15629.11-2003/XG1-2006.

[0085] Another embodiment of the present invention may be implemented in the Otway-Rees protocol, referring to Otway,D. and Ress,O.,"Efficient and timely mutual authentication" ACE OSR, Vol.21,No.1,pp.8-10,Jan. 1987. This protocol is used for identity authentication, and cannot be used in conventional network structures. Specific steps with the method of the present invention cooperating with this protocol are as follows:

[0086] The participants include Alice, Bob and Trent.

[0087] 1] Bob sends a request message to request starting authentication;

[0088] 2] Alice generates a piece of message, which includes an index number, her identity, Bob's identity and a random number, and encrypts this piece of message using the shared key of her and Trent, and then sends the ciphertext together with the index number, the identities of Alice and Bob to Bob;

[0089] 3] Bob generates a piece of message, which includes a new random number, an index number, the identities of Alice and Bob, and encrypts this piece of message using the shared key of him and Trent, and then sends the ciphertext together with the ciphertext of Alice, the index number, and the identities of Alice and Bob to Trent;

[0090] 4] Trent generates a random session key, and then generates two pieces of messages. The first piece of message is to encrypt the random number of Alice and the session key using the shared key of him and Alice. The second piece of message is to encrypt the random number of Bob and the session key using the shared key of him and Bob. Finally, Trent sends the two pieces of messages together with the index numbers to Bob;

[0091] 5] Bob sends the piece of message belonging to Alice as well as the index number to Alice; and

[0092] 6] If all the random numbers are matched and the index number is not changed during the communication process, the authentication succeeds.

[0093] It can be seen that Alice, Bob and Trent respectively implement the subject, the authenticator and the authentication server functions, and this authentication protocol can be implemented in the method of the present invention.

[0094] To sum up, when implementing the method of the present invention in the network structure of a specific type, the authentication carried out by the terminal (subject) and the access controller (authenticator) needs assistance of the server. The terminal can communicate with the access controller and cannot communicate with the server, while the access controller can communicate with the terminal and can also communicate with the server. The terminal, the access controller and the server all participate in the authentication, and the trust relationship is established between the terminal and the access controller directly, which renders security very reliable.

[0095] In addition, the method of the present invention may be implemented in a triple-unit structure, but may be compatible to double-unit double-entity structure. With comparison with Figures 2 and 5, it is known that in the case that there is no authentication server, the implementation of the method of the present invention is totally compatible to the double-unit double-entity network structure. Therefore, the method of the present invention may be implemented in both the double-entity and the triple-entity structure, which may have full adaptability to the existing network structures.

[0096] Besides, when implementing the method according to the present invention, the authentication protocol layer may use existing authentication protocols, or alternatively new authentication protocols may be devised.

[0097] The above embodiments are employed to describe and explain the principles of the present invention. It can be understood that the specific embodiments of the present invention are not limited to those above. Various variations and modifications devised by those skilled in the art without departing from the substance and scope of the present invention are all encompassed within the scope of the present invention. Therefore, the scope of the present invention is defined by the appended claims.

Claims

1. A peer-to-peer access control method of a triple-unit structure, comprising:

    implementing, in a subject, a subject function; implementing, in an authenticator, an authenticator function; and implementing, in an authentication server, an authentication server function:
    setting, in the subject, an authentication method layer of the subject, a peer layer of the subject, an encapsulation layer of the subject and a bottom layer of the subject; setting, in the authenticator, an authentication method layer of the authenticator, an authenticator layer of the authenticator, an encapsulation layer of the authenticator, a bottom layer of the authenticator and a transmission layer of the authenticator; and setting, in the authentication server, an authentication method layer of the authentication server, a peer layer of the authentication server, an encapsulation layer of the authentication server and a transmission layer of the authentication server; and
    implementing, in the authentication method layer of the subject, a function for carrying out, according to an authentication credential, authentication, and implementing, in the bottom layer

of the subject, a function for transmitting data and for controlling, according to a result of the authentication, whether the subject accesses the authenticator; implementing, in the authentication method layer of the authenticator, a function for carrying out, according to an authentication credential, authentication, and implementing, in the bottom layer of the authenticator, a function for controlling, according to a result of the authentication, whether to permit the subject to access the authenticator; and implementing, in the authentication method layer of the authentication server, a function for carrying out, according to an authentication credential, authentication;

implementing an authentication protocol function:

implementing, in the authentication method layer of the subject together with the authentication method layer of the authenticator, the authentication protocol function;

implementing an authentication process:

sending, by the authentication method layer of the authenticator, a request message to the authentication method layer of the subject; and sending, by the authentication method layer of the subject, a response message to the authentication method layer of the authenticator to respond to a valid request message; and

implementing, upon termination of the authentication, access control:

stopping sending, by the authentication method layer of the authenticator when being unable to authenticate the subject according to the response message, the request message and terminating message interaction, and notifying, by the authentication method layer of the authenticator, the bottom layer of the authenticator that the subject is not permitted to access the authenticator; or sending, by the authentication method layer of the authenticator, a failure message to the authentication method layer of the subject, and notifying, by the authentication method layer of the subject, the bottom layer of the subject that the subject is not permitted to access the authenticator; and

stopping sending, by the authentication method layer of the authenticator when determining that the authentication is completed successfully according to the response message, the request message and terminating the message interaction, and notifying, by the authentication method layer of the authenticator, the bottom layer of the authenticator that the subject is permitted to access the authenticator; or sending, by the authentication method layer of the authenticator, a success message to the authentication method layer of the subject, and notifying, by the au-

thentication method layer of the subject, the bottom layer of the subject that the subject is permitted to access the authenticator.

2. The peer-to-peer access control method of a triple-unit structure according to claim 1, wherein the request message sent by the authentication method layer of the authenticator to the authentication method layer of the subject contains a type field, which type field is a field used for indicating a type of the request message; and the response message sent by the authentication method layer of the subject to the authentication method layer of the authenticator contains a type field, which type field corresponds to the type field contained in the request message.

3. The peer-to-peer access control method of a triple-unit structure according to claim 1 or 2, further comprising:

maintaining, as required, the interaction of sending the request message by the authentication method layer of the authenticator and responding to the request message by the authentication method layer of the subject.

4. The peer-to-peer access control method of a triple-unit structure according to claim 1, further comprising:

implementing, in the authentication method layer of the subject together with the authentication method layer of the authenticator and together with the authentication method layer of the authentication server, the authentication protocol function;

sending, by the authentication method layer of the authenticator during the message interaction between the authentication method layer of the subject and the authentication method layer of the authenticator, a request message to the authentication method layer of the authentication server, and sending, by the authentication method layer of the authentication server, a response message to the authentication method layer of the authenticator;

stopping sending, by the authentication method layer of the authenticator when being unable to authenticate the subject according to the response message of the authentication method layer of the subject or according to the response message of the authentication method layer of the authentication server, the request message and terminating the message interaction, and notifying, by the authentication method layer of the authenticator, the bottom layer of the authenticator that the subject is not permitted to access the authenticator; or sending, by the authentica-

tion method layer of the authenticator, the failure message to the authentication method layer of the subject, and notifying, by the authentication method layer of the subject, the bottom layer of the subject that the subject is not permitted to access the authenticator; and

stopping sending, by the authentication method layer of the authenticator when determining that the authentication is completed successfully according to the response message of the authentication method layer of the subject or according to the response message of the authentication method layer of the authentication server, the request message and terminating the message interaction, and notifying, by the authentication method layer of the authenticator, the bottom layer of the authenticator that the subject is permitted to access the authenticator; or sending, by the authentication method layer of the authenticator, the success message to the authentication method layer of the subject, and notifying, by the authentication method layer of the subject, the bottom layer of the subject that the subject is permitted to access the authenticator.

5. The peer-to-peer access control method of a triple-unit structure according to claim 4, wherein the request message sent by the authentication method layer of the authenticator to the authentication method layer of the subject contains a type field, which type field is a field used for indicating a type of the request message; and the response message sent by the authentication method layer of the subject to the authentication method layer of the authenticator contains a type field, which type field corresponds to the type field contained in the request message; and the request message sent by the authentication method layer of the authenticator to the authentication method layer of the authentication server contains a type field, which type field is a field used for indicating a type of the request message; and the response message sent by the authentication method layer of the authentication server to the authentication method layer of the authenticator contains a type field, which type field corresponds to the type field contained in the request message.

6. The peer-to-peer access control method of a triple-unit structure according to claim 4 or 5, further comprising:

maintaining, as required, the interaction of sending the request message by the authentication method layer of the authenticator and responding to the request message by the authentication method layer of the subject; and
maintaining, as required, the interaction of sending the request message by the authentication

method layer of the authenticator and responding to the request message by the authentication method layer of the authentication server.

7. The peer-to-peer access control method of a triple-unit structure according to claim 1 or 4, wherein the subject is a terminal; the authenticator is an access controller; and the authentication server is a server.

Fig.1

Terminal		Access controller

Authentication method layer
Peer layer
Encapsulation layer
Bottom layer

Authentication method layer
Authenticator layer
Encapsulation layer
Bottom layer

Fig.2

Terminal   Access controller   Server

Authentication method layer
Peer layer
Encapsulation layer
Bottom layer

Authenticator layer	
Encapsulation layer	
Bottom layer	Transmission layer

Authentication method layer
Authenticator layer
Encapsulation layer
Transmission Layer

Fig.3

Terminal   Access controller   Server

401 Request

402 Response

403 Request

404 Response

405 Request

406 Response

407 Success/failure

Fig.4

Terminal (corresponding to subject)	Access controller (corresponding to authenticator)	Server (corresponding to authentication server)

Authentication method layer
Peer layer
Encapsulation layer
Bottom layer

Authentication method layer	
Authenticator layer	
Encapsulation layer	
Bottom layer	Transmission layer

Authentication method layer
Peer layer
Encapsulation layer
Transmission Layer

Fig.5

ASUE   AE   ASE

601 Authentication activation packet

602 Access authentication request packet

603 Certificate authentication request packet

604 Certificate authentication response packet

605 Access authentication response packet

Fig.6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2007/070171

A. CLASSIFICATION OF SUBJECT MATTER
H04L 29/06 (2006.01) i
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED
Minimum documentation searched (classification system followed by classification symbols)
IPC: H04L; H04B; H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
CNPAT; CNKI; WPI; EPODOC; PAJ; IEEE: AAA, authenticat+, authoriz+, peer, server, control, access, NAS, RADIUS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 1567868 A (HUAWEI TECHNOLOGIES CO. LTD.) 19 Jan. 2005 (19.01.2005) page 3 line 9 to page 4 line 1, page 4 line 26 to page 6 line 10, page 8 line 19 to page 9 line 1, page 10 line 26 to page 11 line 11 in the description, Fig. 7, 10	1-7
A	CN 1539106 A (NOKIA CORP.) 20 Oct. 2004 (20.10.2004) the whole document	1-7
A	CN 1765082 A (CISCO TECHNOLOGY INC.) 26 Apr. 2006 (26.04.2006) the whole document	1-7

☒ Further documents are listed in the continuation of Box C.	☒ See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	
"E" earlier application or patent but published on or after the international filing date	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"L" document which may throw doubts on priority claim (S) or which is cited to establish the publication date of another citation or other special reason (as specified)	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
10 Sep. 2007 (10.09.2007)	**27 Sep. 2007 (27.09.2007)**
Name and mailing address of the ISA/CN The State Intellectual Property Office, the P.R.China 6 Xitucheng Rd., Jimen Bridge, Haidian District, Beijing, China 100088 Facsimile No. 86-10-62019451	Authorized officer LI, Nan Telephone No. (86-10)82755431

Form PCT/ISA/210 (second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT

	International application No.
	PCT/CN2007/070171

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2004098612 A1 (MEDNOVUS, INC.) 20 May 2004(20.05.2004) the whole document	1-7
A	EP 1708447 A1 (BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY) 04 Oct. 2006(04.10.2006) the whole document	1-7

Form PCT/ISA/210 (continuation of second sheet) (April 2007)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2007/070171

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 1567868 A	19.01.2005	CN 1319337 C	30.05.2007
CN 1539106 A	20.10.2004	WO 03007102 A	23.01.2003
		AU 2002319555 A	29.01.2003
		US 2003028763 A	06.02.2003
		EP 1415212 A	06.05.2004
CN 1765082 A	26.04.2006	US 2004168054 A	26.08.2004
		WO 2004077750 A	10.09.2004
		AU 2004214799 A	10.09.2004
		CA 2517474 A	10.09.2004
		EP 1597866 A	23.11.2005
US 2004098612 A1	20.05.2004	KR 20040040709 A	13.05.2004
EP 1708447 A1	04.10.2006	WO 2006103386 A	05.10.2006

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

• CN 200610105203 **[0001]**

Non-patent literature cited in the description

• **Otway,D. ; Ress,O.** Efficient and timely mutual authentication. *ACE OSR,* January 1987, vol. 21 (1), 8-10 **[0085]**